Appendix D. List of Programs

Figure 10. Program of Record Transition Timeline

IPv6 Survey D-1. Tactical Data Network

1. Program Name	Tactical Data Network
2. System/product identification	
a. Program Manager	LtCol J. D. Wilson
b. Program Group	MAGTF C4ISR
c. Milestone reached	C
3. POCs: (program and technical POCs, telephone number, address, email)	Project Officer: Capt C. J. Buchanan Team Leader: Ms. T. Conte
4. Identify Operating System(s) (OS) used	Windows NT Server 4.0
5. Identify applications used. All COTS and GOTS software should be identified.	Service Pack 6.A for NT 4.0 Video Driver: Matrox Millennium G200 Norton AntiVirus 7.6 Netscape Communicators 6.2 Walusoft TFTPSuitePro2000 3.6 Network Time Protocol (XNTP 3.5) Client/Server Window Service For Unix 1.0 Tera Term Pro 2.3 Printer Driver Tape Driver Norton SpeedDisk 5.0 Adobe Acrobat Reader 5.0 MetaIP 4.1 Enterprise Edition (with SP4) Internet Explorer 5.5SP2 NT Option Pack 4 (IIS 4.0 & FTP) SiteNet MultiLink 1.5 COE Kernel 3.4 HPOV NNM 6.1 DMS GWS 2.0.3 (Microsoft Exchange 5.5) Veritas Backup Exec 8.0.3166 Veritas Backup Exchange Module Install Shield Script 1.0 Norton Ghost 6.0 NNM-RME Integration Package CiscoWorks 2000 Roxio Easy CD Creator Power Console Plus U-Promote 4.61

	Card Wizzard 5.20.04
6. Define how <u>each</u> application identified above uses Internet Protocol (IP):	
a. Is Source Code available for this application? If so, evaluating this code with tools described in section 5.3 will help answer b and c below.	No to all
b. Define how IP calls are implemented (sockets, API). Identify whether applications use embedded protocol stacks or rely on OS function calls and protocol stacks. Applications with embedded protocol stacks may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below. See Chapter II.	TDN uses multiple COTS software products. Moving to Windows 2003 in order to facilitate IPv6 will require a new software baseline, so this will not be applicable to an upgraded system. It is not known how IP calls are implemented in the COTS software.
c. Define how IP addresses are obtained (static IP addresses, DHCP, BOOTP, other). Identify use of hard-coded IP addresses. Applications with hard-coded IP addresses may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below.	IP addresses are obtained via DHCP (NIPRNET), but the TDN DDS system supports DHCP.
7. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6. IPv6 capability is expected by 2008. See Chapter IV.	Routers and switches and NICs will have to be upgraded, and a new software baseline will need to be developed.
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture. New and enhanced capabilities afforded by IPv6 include extension headers, mobile IPv6, IPSec, Flow Labels, unicast/multicast/anycast addressing, and address autoconfiguration. See Chapter III.	TDN will act as the conduit for tactical data traffic, so this would be pertinent to the system only in context of the applications it is supporting. Since this equates to all tactical data systems, all these capabilities will be leveraged as appropriate. They should all be available unless system performance is degraded.
8. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation. Technical dependencies include OS support for IPv6, hard-coded IPv4 implementation in applications, reliance on COTS databases and applications, dependency on external network	This is not well known at this time. We have hardware upgrades planned in FY-05-07 that will ensure our routers and switches are ready, the software should be in place by then also. Dependencies that we know of are: Operating System Routers & Switches Operator Training COTS applications (unknown)

services, etc.	Encryption Devices
b. Describe external systems with which your system is known to communicate using IP.	DTC, DISN, SIPRNet, NIPRnet
9. Programmatic impact(s):	
a. Development schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed development if possible. Full IPv6 capability is expected by 2008. b. Deployment/fielding/upgrade/ retrofit schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed upgrades if possible. Full IPv6 capability is expected by 2008.	(b)(7)(E)
c. Cost schedule. Identify additional funding required to achieve initial and objective IPv6 capabilities identified in the schedules above. Only costs beyond what is already programmed for tech refresh or upgrade should be identified.	$5.3M will be needed to upgrade to Windows Server 2003. (b)(7)(E) (b)(7)(E) (b)(7)(E). Hardware upgrades will cost about $26M. Total cost is $42M, but only 5.3 that is not already budgeted.
10. Define technical and programmatic risks. Identify any known impediments to IPv6 transition. See Chapter V.	$5.3M in FY-05 is not budgeted for. This includes modifying the schoolhouse also.
11. Recommendations/Comments	
12. Is this program a good candidate to become a Marine Corps IPv6 "early adopter"?	Yes. Relatively low number of systems (507) with large return on investment (all tactical data comms). Compressing time to change over could yield economies of scale.

IPv6 Survey D-2. EFV (C)

EFV (C) Program of Record and System IPv6 Checklist							
1. Software Support Activity:							
PG:	Direct Reporting Program Manager (DRPM) Advanced Amphibious Assault (AAA)			PM Phone:	(703) 492-3300		
PM:	Colonel Michael M. Brogan			PM Email:	BroganMM@efv.usmc.mil		
Prime Support Contractor:	General Dynamics Amphibious Systems						
Enter ORGANIC if the PM Shop maintains the application with organic resources (Civilians and/or Marines)							
2. System/product Identification:							
a. System Name:	Expeditionary Fighting Vehicle Command Variant				b. Acronym:	EFV(C)	
c. Version #:	N/A	d. DADMS ID #:	N/A	e. DARS ID#:	N/A	f. MSTAR ID #:	N/A
3. Program Status:							
a. Current MS:	B	b. MS Date:	Nov 2000	c. IATO Date:	FY 2007	d. ATO Date:	FY 2007

4. Identify applications used: (Add more lines as required, see Type Code legend below)

Application Name	Purpose	Type	Version
Windows NT Workstation	C2PC Operations	C	4.0
Windows 2000	Vehicle Operations	C	2000
Windows NT Server	C2PC Gateway	C	4.0 w/SP6a
Solaris	AFATDS Operations	C	2.5.1
Solaris	IOS(V)2 Operations	C	2.7
VxWorks	Vehicle Operations	C	5.4.2
AFATDS	AFATDS Operations	G	6.3.1 SP4
X Windows	Solaris Unix Operations	C	N/A
IOS (V)2	IOS(V)2 Operations	G	3.6
C2PC	C2PC Operations	G	5.9.0.3
Effects Management Tool	Allows track dissemination between AFATDS, IOS, and C2PC	G	6.3.1
EPLRS Network Manager	EPLRS Operation	G	4.0.2
Microsoft Internet Explorer	Web application	C	5.0
Adobe Acrobat Reader	Review .pdf files	C	4.0
Altiris Carbon Copy	Remote control application—provides the tools needed to remotely administer the EFV network from any onboard Data Processing Unit	C	5.6
Cryptek Secure Communications Printer Services	TS-21 Printer/Fax/Scanner Operations	C	N/A
GNU Ghostscript	allows UNIX machines to print to the Cryptek printer	C	7.04

Ghostgum Software GSview	allows UNIX machines to print to Cryptek Printer	C	4.2
Hummingbird Exceed	permits applications, normally available only on UNIX workstations, to be readily accessed from enterprise desktops	C	7.0
HP OpenView Network Node Manager	provides a variety of real-time views of your network status and alerts you to network problems remotely by pager or e-mail before they escalate into expensive downtime events	C	6.1
Internet Locator Server	Provides white board capablity	C	2.0
Leutron Vision Software Development Suite	Viewing live video from the Vehicle Thermal Viewer	C	1.93.001
Microsoft Exchange 2000 Enterprise Server	TDN Exchange Services	C	2000
TimeServ	Provides network time to all Data Processing Units (DPU's)	C	1.5
Microsoft Windows Services for UNIX®	Network File System	C	2.0
Microsoft Windows NetMeeting	can be used to remotely access computers for multiple purposes, hold a videoconference, transfer files and conduct a private chat	C	3.01
Redmon Redirction Port Monitor	allows printing from UNIX to NT	C	N/A
Symantec Norton Anti Virus	Network Virus Protection	C	2000
Symantec Norton Ghost Corporate Edition	Image System Software	C	7.5
3Com Boot Services OEM	Provides remote network booting and rebooting	C	1.02
WinZip	File compression	C	8.0
JAVA Run Time	JAVA Operations	C	N/A
Ground Tactical Communications Services	SP-TCIM/TacLink 3000 Operations	G	2.0.0.5
Test Utilities Client Processor Manager	Spray Cool Test Manager	G	3.0a
Test Utilities	Spray Cool Test Manager	G	3.0a
Mobility, Power Management, and Auxilary (MPA)	EFV Unique Software for Vehicle Operations	G	N/A
Control and Displays (C&D)	EFV Unique Software for Vehicle Operations	G	N/A

Type Code Legend:

G = Government Off-the-Shelf **C** = Commercial Off-the-Shelf **MC** = COTS Modified by Government Contract but still

S = Shareware **F** = Freeware available to the public.

5. Identify reliance on IPv4: [Appendix A, Chapter 2]

a. Define how IPv4 is implemented preventing IPv6 capability: (Database fields; hard-coded addressing; proprietary protocol implementation; IPv4 loopback addresses; reliance on non-IPv6 OS, COTS, or GOTS)	1) All COTS applications are dependent upon industry dual stack IPv4 and IPv6 implementation. 2) Ethernet routers and switches are dependent upon industry dual stack IPv4 and IPv6 implementation. 3) The EFV will upgrade from Windows NT Server to a dual stack IPv4 and IPv6 capable server as soon as the Marine Corps upgrades the software drivers in the Ground Tactical Communications Services (GTCS) software required to support the interoperability between the operating system and the SP-TCIM/TacLink 3000 modems. 4) EPLRS and VDC-500 upgrades are dependent upon the Marine Corps IPv6 implementation to support the MAGTF architecture.
b. Define how IP addresses are obtained: (static IP addresses, DNS lookup, DHCP, BOOTP, other)	Static IP addresses. EFV unique MPA and C&D software use hard-coded IP addresses and will require further development, testing, and certification to support dual stack IPv4 and IPv6 functionality.
6. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6.	1) EFV unique MPA and C&D software will require software code modification to support dual stack IPv4 and IPv6 functionality. 2) C2PC software code modification will be required to support dual stack IPv4 and IPv6 functionality (Marine Corps responsibility). EFV will be required to integrated and test this new functionality. 4) Upgrades will be required to support dual stack IPv4 and IPv6 routing functionality for all Ethernet switches, Ethernet routers, EFV unique displays, EPLRS Radios, VDC-500, and SP-TCIM/TacLink 3000 modems. 5) AFATDS software code modification will be required to support dual stack IPv4 and IPv6 routing functionality (Army/Marine Corps responsibility). EFV will be required to integrated and test this new functionality. 6) IOS (V2) software code modification will be required to support dual stack IPv4 and IPv6 routing functionality (Marine Corps responsibility). EFV will be required to integrated and test this new functionality. 5) EFV will be required to upgrade, integrate, and test all operating systems and applications to a dual stack IPv4 and IPv6 capability.
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture (i.e. stacked headers, site/link local addressing, mobile IPv6, IPSec, unicast/multicast/anycast, stateless autoconfiguration). [Appendix A, Chapter 3]	This depends on the modification of the Marine Air Ground Task Force (MAGTF) architecture migration to support both IPv4 and IPv6 routing functionality.
7. Dependencies:	

a. Describe technical dependencies that will impact the system with IPv6 implementation, i.e. processor or memory constraints, APIs, COE, etc.	1) All COTS applications are dependent upon industry dual stack IPv4 and IPv6 implementation. 2) Ethernet routers and switches are dependent upon industry dual stack IPv4 and IPv6 implementation. 3) The EFV will upgrade from Windows NT Server to a dual stack IPv4 and IPv6 capable server as soon as the Marine Corps upgrades the software drivers in the Ground Tactical Communications Services (GTCS) software required to support the interoperability between the operating system and the SP-TCIM/TacLink 3000 modems. 4) EPLRS and VDC-500 upgrades are dependent upon the Marine Corps IPv6 implementation to support the MAGTF architecture.
b. Describe logistical dependencies external to your system, i.e. interrelated programs (C2PC, NCES, TDN, etc.) Upper Layer Protocols and applications.	AFATDS, IAS, IOW, DACT, GCCS, TBMCS
8. Programmatic impact(s):	
a. Schedule for system to be dual-stack and full IPv6 capable using current Development Schedule. Include deployment, fielding, upgrade, and retrofit milestones.	The EFV(C) is under development and is expected to obtain a Milestone C decision in late FY05 and reach IOC in FY08. DRPM AAA's technology migration plan will begin IPv6 development in FY05 and expect to be fully capable of IPv4 and IPv6 by FY08. However, a dual stack IPv4 and IPv6 capability cannot be achieved without Army and/or Marine Corps upgrades to AFATDS, IOS(V2), C2PC, and GTCS software.
(1) Cost schedule – additional funding required (deficiency) to achieve initial and objective IPv6 capabilities in 8a that is not already budgeted, such as for tech refresh or upgrade. [Section 5.3 of the Transition Plan]	No additional funding required.
b. Accelerated schedule for system to be dual-stack and full IPv6 capable if current Development Schedule does not meet the goal of IPv6 capable by 2008. Include deployment, fielding, upgrade, and retrofit milestones.	Not Applicable
(1) Cost schedule – additional funding required (deficiency) to achieve initial and objective IPv6 capabilities in 8b that is not already budgeted, such as for tech refresh or upgrade. [Section 5.3 of the Transition Plan]	No additional funding required.
9. Define technical and programmatic risks.	
An IPv4 and IPv6 capability cannot be achieved without Army and/or Marine Corps upgrades to AFATDS, IOS(V2), C2PC, GTCS software, EPLRS, and the VDC-500.	
10. Define Risk Mitigation Strategy for items identified in block 9.	
Can only be addressed by the USMC	
11. Can this system become a Marine Corps representative "early adopter"? (Yes / No)	No

IPv6 Survey D-3. EFV (P)

EFV (P) Program of Record and System IPv6 Checklist			
1. Software Support Activity:			
PG:	Direct Reporting Program Manager (DRPM) Advanced Amphibious Assault (AAA)	PM Phone:	(703) 492-3300
PM:	Colonel Michael M. Brogan	PM Email:	BroganMM@efv.usmc.mil
Prime Support Contractor:	General Dynamics Amphibious Systems		
Enter ORGANIC if the PM Shop maintains the application with organic resources (Civilians and/or Marines)			

2. System/product Identification:							
a. System Name:	Expeditionary Fighting Vehicle Personnel Variant				b. Acronym:	EFV(P)	
c. Version #:	N/A	d. DADMS ID #:	N/A	e. DARS ID#:	N/A	f. MSTAR ID #:	N/A

3. Program Status:							
a. Current MS:	B	b. MS Date:	Nov 2000	c. IATO Date:	FY 2007	d. ATO Date:	FY 2007

4. Identify applications used: (Add more lines as required, see Type Code legend below)

Application Name	Purpose	Type	Version
Windows 2000	Vehicle Operations	C	2000
Windows NT Server	C2PC Gateway	C	4.0 w/SP6a
VxWorks	Vehicle Operations	C	5.4.2
C2PC	C2PC Operations	G	5.9.0.3 SP4
JAVA Run Time	JAVA operations	C	N/A
Mobility, Power Management, and Auxilary (MPA)	EFV Unique Software for Vehicle Operations	G	N/A
Control and Displays (C&D)	EFV Unique Software for Vehicle Operations	G	N/A
Fire Control (FC)	EFV Unique Software for Vehicle Weapon Employment	G	N/A
Altiris Carbon Copy	Remote control application—provides the tools needed to remotely administer the EFV network from any onboard Data Processing Unit	C	5.6
Ground Tactical Communications Services	SP-TCIM/TacLink 3000 Operations	G	2.0.0.5

Type Code Legend:

G = Government Off-the-Shelf **C** = Commercial Off-the-Shelf **MC** = COTS Modified by Government Contract but still available to the public.

S = Shareware **F** = Freeware

5. Identify reliance on IPv4: [Appendix A, Chapter 2]	
a. Define how IPv4 is implemented preventing IPv6 capability: (Database fields; hard-coded addressing; proprietary protocol implementation; IPv4 loopback addresses; reliance on non-IPv6 OS, COTS, or GOTS)	MPA, C&D, and FC EFV unique software use OS function calls and protocol stacks. All COTS and GOTS products are not under control of the EFV program office.

b. Define how IP addresses are obtained: (static IP addresses, DNS lookup, DHCP, BOOTP, other)	Static IP addresses. EFV unique MPA, C&D, and FC software use hard-coded IP addresses and will require further development, testing, and certification to support dual stack IPv4 and IPv6 functionality.
6. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6.	1) EFV unique MPA, C&D, and FC software will require software code modification to support dual stack IPv4 and IPv6 functionality. 2) C2PC software code modification will be required to support dual stack IPv4 and IPv6 functionality (Marine Corps responsibility). EFV will be required to integrate and test this new functionality. 4) Upgrades will be required to support dual stack IPv4 and IPv6 routing functionality for all Ethernet switches, EFV unique displays, EPLRS Radios, VDC-500, and SP-TCIM/TacLink 3000 modems. 5) EFV will be required to upgrade, integrate, and test all operating systems and applications to a dual stack IPv4 and IPv6 capability.
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture (i.e. stacked headers, site/link local addressing, mobile IPv6, IPSec, unicast/multicast/anycast, stateless autoconfiguration). [Appendix A, Chapter 3]	This depends on the modification of the Marine Air Ground Task Force (MAGTF) architecture migration to support both IPv4 and IPv6 routing functionality.
7. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation, i.e. processor or memory constraints, APIs, COE, etc.	1) All COTS applications are dependent upon industry dual stack IPv4 and IPv6 implementation. 2) Ethernet switches are dependent upon industry dual stack IPv4 and IPv6 implementation. 3) The EFV will upgrade from Windows NT Server to a dual stack IPv4 and IPv6 capable server as soon as the Marine Corps upgrades the software drivers in the Ground Tactical Communications Services (GTCS) software required to support the interoperability between the operating system and the SP-TCIM/TacLink 3000 modems. 4) EPLRS and VDC-500 upgrades are dependent upon the Marine Corps IPv6 implementation to support the MAGTF architecture.
b. Describe logistical dependencies external to your system, i.e. interrelated programs (C2PC, NCES, TDN, etc.) Upper Layer Protocols and applications.	IOS, DACT, GCCS
8. Programmatic impact(s):	

a. Schedule for system to be dual-stack and full IPv6 capable using current Development Schedule. Include deployment, fielding, upgrade, and retrofit milestones.	The EFV(P) is under development and is expected to obtain a Milestone C decision in late FY05 and reach IOC in FY08. (b)(7)(E)
(1) Cost schedule – additional funding required (deficiency) to achieve initial and objective IPv6 capabilities in 8a that is not already budgeted, such as for tech refresh or upgrade. [Section 5.3 of the Transition Plan]	No additional funding required.
b. Accelerated schedule for system to be dual-stack and full IPv6 capable if current Development Schedule does not meet the goal of IPv6 capable by 2008. Include deployment, fielding, upgrade, and retrofit milestones.	Not Applicable
(1) Cost schedule – additional funding required (deficiency) to achieve initial and objective IPv6 capabilities in 8b that is not already budgeted, such as for tech refresh or upgrade. [Section 5.3 of the Transition Plan]	No additional funding required.

9. Define technical and programmatic risks.
(b)(7)(E) (b)(7)(E)

10. Define Risk Mitigation Strategy for items identified in block 9.
Can only be addressed by the USMC

11. Can this system become a Marine Corps representative “early adopter”? (Yes / No)	No

IPv6 Survey D-4. CAC2S

1. Program Name	Common Aviation Command and Control System
2. System/product identification	CAC2S
a. Program Manager	PM Operations Centers
b. Program Group	Product Group 11, Battlespace Management and Air Defense Systems (BMADS)
c. Milestone reached	B
3. POCs: (program and technical POCs, telephone number, address, email)	Team Lead: LtCol Jeff Speights, (703)432-4104, speightsjs@mcsc.usmc.mil System Engineer: Maj Todd Emo, (703)432-4086, emotr@mcsc.usmc.mil
4. Identify Operating System(s) (OS) used	VxWorks 5.4, Win2000, Solaris
5. Identify applications used. All COTS and GOTS software should be identified.	**GOTS:** SSDS MK II MTS **COTS:** AccessNet Ternion- FLAMES Gallium InterMAPhics Various MS Products Exceed (Unix emulation)
6. Define how each application identified above uses Internet Protocol (IP):	
a. Is Source Code available for this application? If so, evaluating this code with tools described in section 5.3 will help answer b and c below.	GOTS – yes; COTS –no.
b. Define how IP calls are implemented (sockets, API). Identify whether applications use embedded protocol stacks or rely on OS function calls and protocol stacks. Applications with embedded protocol stacks may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below. See Chapter II.	Sockets The COTS products use O/S function calls.
c. Define how IP addresses are obtained (static IP addresses, DHCP, BOOTP, other). Identify use of hard-coded IP addresses. Applications with hard-coded IP addresses may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below.	The system uses both DHCP and Static IP addresses under administrator control. Certain radar interfaces currently use hard-coded IP addresses.
7. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6. IPv6 capability is expected by 2008.	Dual Capability: o Replace system routers and switches to obtain full IPv6 capability external to this system.

See Chapter IV.	Full Capability: o Replace system routers and switches with IPv6 capable H/W o Significant modification to approximately 6 interface software SCIs o Transition to next version of O/Ss that support IPv6
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture. New and enhanced capabilities afforded by IPv6 include extension headers, mobile IPv6, IPSec, Flow Labels, unicast/multicast/anycast addressing, and address autoconfiguration. See Chapter III.	None at this time.
8. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation. Technical dependencies include OS support for IPv6, hard-coded IPv4 implementation in applications, reliance on COTS databases and applications, dependency on external network services, etc.	VxWorks support for IPv6. Win2000 (DII-COE O/S) support for IPv6 Transition of external systems identified in 8.b.
b. Describe external systems with which your system is known to communicate using IP.	SIPRNet NIPRNet GCCS I3/IAS AFATDS TBMCS CEC CDLMS EPLRS
9. Programmatic impact(s):	
a. Development schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed development if possible. Full IPv6 capability is expected by 2008.	Detailed schedule being analyzed by development prime contractor. (b)(7)(E)
b. Deployment/fielding/upgrade/ retrofit schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed upgrades if possible. Full IPv6 capability is expected by 2008.	Detailed schedule being analyzed by development prime contractor. (b)(7)(E)

c. Cost schedule. Identify additional funding required to achieve initial and objective IPv6 capabilities identified in the schedules above. Only costs beyond what is already programmed for tech refresh or upgrade should be identified.	Unknown at this time. Clearly involves some hardware replacements and software modifications, as well as dependencies on several other DoD systems. Prime contractor is currently developing a cost impact.
10. Define technical and programmatic risks. Identify any known impediments to IPv6 transition. See Chapter V.	IPv6 implementation requirements for security re-certification.
11. Recommendations/Comments	
12. Is this program a good candidate to become a Marine Corps IPv6 "early adopter"?	No. Critical dependencies on other Navy and Joint programs limit Marine Corps flexibility.

IPv6 Survey D-5. GATOR

1. Program Name	**Ground Air Task Oriented Radar (GATOR)**
2. System/product identification	Not assigned
a. Program Manager	Mr. John McGough, (703) 432-4217
b. Program Group	BMADS Radar
c. Milestone reached	MSA, MSB scheduled for DEC04
3. POCs: (program and technical POCs, telephone number, address, email)	Capt. Kenneth VanZandt, (703)432-4246, vanzandtkl@mcsc@usmc.mil GySgt Hondo Shaver, (703) 432-4228, shaverhj@mcsc.usmc.mil
4. Identify Operating System(s) (OS) used	TBD
5. Identify applications used. All COTS and GOTS software should be identified.	TBD
6. Define how each application identified above uses Internet Protocol (IP):	
a. Is Source Code available for this application? If so, evaluating this code with tools described in section 5.3 will help answer b and c below.	Pre MSB no code has been written. This system will be fielded after FY08. All requirements for IPV6 should be addressed during the system design and development process.
b. Define how IP calls are implemented (sockets, API). Identify whether applications use embedded protocol stacks or rely on OS function calls and protocol stacks. Applications with embedded protocol stacks may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below. See Chapter II.	UNK
c. Define how IP addresses are obtained (static IP addresses, DHCP, BOOTP, other). Identify use of hard-coded IP addresses. Applications with hard-coded IP addresses may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below.	UNK
7. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6. IPv6 capability is expected by 2008. See Chapter IV.	UNK
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture. New and enhanced capabilities afforded by IPv6 include extension headers, mobile IPv6,	UNK

IPSec, Flow Labels, unicast/multicast/anycast addressing, and address autoconfiguration. See Chapter III.	
8. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation. Technical dependencies include OS support for IPv6, hard-coded IPv4 implementation in applications, reliance on COTS databases and applications, dependency on external network services, etc.	UNK
b. Describe external systems with which your system is known to communicate using IP.	UNK
9. Programmatic impact(s):	
a. Development schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed development if possible. Full IPv6 capability is expected by 2008.	This system will be fielded after FY08. All requirements for IPV6 should be addressed during the system design and development process.
b. Deployment/fielding/upgrade/ retrofit schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed upgrades if possible. Full IPv6 capability is expected by 2008.	UNK
c. Cost schedule. Identify additional funding required to achieve initial and objective IPv6 capabilities identified in the schedules above. Only costs beyond what is already programmed for tech refresh or upgrade should be identified.	UNK
10. Define technical and programmatic risks. Identify any known impediments to IPv6 transition. See Chapter V.	UNK
11. Recommendations/Comments	None
12. Is this program a good candidate to become a Marine Corps IPv6 “early adopter”?	No, The system is not scheduled to field until after FY08

IPv6 Survey D-6. Firefinder Radar System

1. Program Name	**Firefinder Radar System, AN/TPQ-36 (V)8 (USA), AN/TPQ-46A (USMC)**
2. System/product identification	AN/TPQ-36 (V)8 (US Army), AN/TPQ-46A (USMC)
a. Program Manager	Mr. John McGough, (703) 432-4217
b. Program Group	BMADS Radar
c. Milestone reached	Sustainment
3. POCs: (program and technical POCs, telephone number, address, email)	GySgt Hondo Shaver, (703) 432-4228, shaverhj@mcsc.usmc.mil POC Mary Ann Pursley, DSN 639-3651, Comm (580) 442-6351.
4. Identify Operating System(s) (OS) used	Linux, Sun Solaris, Windows
5. Identify applications used. All COTS and GOTS software should be identified.	Red Hat Linux, Sun Solaris, FFPAS
6. Define how each application identified above uses Internet Protocol (IP):	
a. Is Source Code available for this application? If so, evaluating this code with tools described in section 5.3 will help answer b and c below.	YES, The source code for this system is owned and maintained by the US Army's Fort Sill Software Engineering (FSSE) Center, Ft Sill, Oklahoma. POC Mary Ann Pursley, DSN 639-3651, Comm (580) 442-6351.
b. Define how IP calls are implemented (sockets, API). Identify whether applications use embedded protocol stacks or rely on OS function calls and protocol stacks. Applications with embedded protocol stacks may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below. See Chapter II.	(b)(7)(E)
c. Define how IP addresses are obtained (static IP addresses, DHCP, BOOTP, other). Identify use of hard-coded IP addresses. Applications with hard-coded IP addresses may require development, testing and certification to support IPv6. Identify this effort in items 7, 8, and 9 below.	(b)(7)(E)
7. Technical impact of transition to IPv6:	
a. Describe what needs to be done to the system to achieve initial dual stack capability and/or full transition to IPv6. IPv6 capability is expected by 2008. See Chapter IV.	(b)(7)(E)
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture. New and enhanced capabilities afforded by IPv6 include extension headers, mobile IPv6,	(b)(7)(E)

IPSec, Flow Labels, unicast/multicast/anycast addressing, and address autoconfiguration. See Chapter III.	
8. Dependencies:	
a. Describe technical dependencies that will impact the system with IPv6 implementation. Technical dependencies include OS support for IPv6, hard-coded IPv4 implementation in applications, reliance on COTS databases and applications, dependency on external network services, etc.	(b)(7)(E)
b. Describe external systems with which your system is known to communicate using IP.	(b)(7)(E)
9. Programmatic impact(s):	
a. Development schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed development if possible. Full IPv6 capability is expected by 2008.	(b)(7)(E)
b. Deployment/fielding/upgrade/ retrofit schedule for dual-stack and full IPv6 implementation. The schedule should match currently programmed upgrades if possible. Full IPv6 capability is expected by 2008.	(b)(7)(E)
c. Cost schedule. Identify additional funding required to achieve initial and objective IPv6 capabilities identified in the schedules above. Only costs beyond what is already programmed for tech refresh or upgrade should be identified.	(b)(7)(E)
10. Define technical and programmatic risks. Identify any known impediments to IPv6 transition. See Chapter V.	(b)(7)(E)
11. Recommendations/Comments	None
12. Is this program a good candidate to become a Marine Corps IPv6 "early adopter"?	(b)(7)(E) (b)(7)(E)